- Title **INFORMATION SECURITY OFFICIAL**
- Creation
  - Date June 3, 2001
  - Author Patricia Kuhar of DOIT
  - Email address pkuhar@doit.ca.gov
- Revision
  - Date November 30, 2001
  - Author Patricia Kuhar of DOIT
  - Phone number 916-445-6201
  - Email address pkuhar@doit.ca.gov

I. Introduction

This template is designed to provide covered entities, who are required or who wish to comply with the Health Insurance Portability and Accountability Act (HIPAA) administrative requirements in designating an Information Security Official, with duties and responsibilities for this position.

II. Purpose

Describe the basic requirements expected of the Information Security Official who is responsible for the development and implementation of the covered entity's policies and procedures.

A. Specific HIPAA requirements/standards addressed

HIPAA rules require covered entities to establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and availability of information.

Federal Rules under HIPAA require the establishment of an assigned security responsibility (which will be implemented through an Information Security Official, to handle Information Security practices by developing policy and procedures, establishing training, and compliance processing. A separate function for addressing complaints and whistleblower issues may be a part of the duties of this position (refer to the Contact Person template and the Privacy Official template for complaint and whistleblower issues).

B. Areas in which this template should be utilized

This template sets forth job duties and responsibilities of the Information Security Official position.

This template does not address which classification position or salary range to use for the Information Security Official. Each covered entity needs to develop a statement of duties, responsibilities, and requirements for the Information Security Official following appropriate personnel guidelines.

C. Pertinent References

The pertinent reference is: Federal Register dated 8/12/98, 63 Code of Federal Regulations 43242, on Standards for Information Security of Individually Identifiable Health Information. The Notice of Proposed Rule Making (NPRM) describes how to comply with the HIPAA requirement for use and disclosure of individually identifiable health information. The administrative requirement for a covered entity to designate an assigned security responsibility (here implemented via an Information Security Official) is cited in the proposed Security Rule in 142.308(b)(1)). For all covered entities, the required date of compliance is within (24) months of the effective date of the final HIPAA Security Rules.

Under Government Code Section 11771, and the State Administrative Manual Sections 4840.2 and 4841.1, each agency must have an Information Security Officer (ISO) to oversee agency compliance with policies and procedures regarding the security of information assets. The ISO, to avoid conflicts of interest:

- must be responsible to the agency director
- must be of a sufficiently high level classification to execute responsibilities in an effective and independent manner
- should not have direct responsibility for information processing, information security functions or agency programs that employ confidential information (exception: state data centers).

Security Rule 142.310(10) HIPAA also contains new standards for safeguarding the privacy and security of health information. Therefore, the development of policies for safeguarding the privacy and security of health records is a fundamental and indispensable part of HIPAA implementation that must accompany or precede the expansion or standardization of technology for recording or transmitting health information.

III. Assumptions

Information Security concerns grow as technology increases access to Individually Identifiable Health Information (IIHI). Health issues such as mental health, substance abuse, sexually transmitted diseases, and genetic information create a heightened awareness of the need for Information Security.

The HIPAA Security Rules were designed to protect IIHI against unauthorized use or disclosure and reasonably anticipated threats or hazards to the security or integrity of information.

All ongoing activities related to the development, implementation, maintenance, and adherence to the entity's policy and procedures covering information security must be addressed.

The HIPAA Rules contain a set of requirements with implementation features that covered entities must include in their operations to ensure that health information in electronic form pertaining to an individual remains secure from unauthorized access or unauthorized use.

Federal and State laws and regulations exist to protect citizens by limiting the release of information based on the requestor, the type of information, and the use of that information.

IV. Pre-requisites

The rules for Information Security of IIHI require that a covered entity designate an Information Security Official who is responsible for the development and implementation of policies and procedures relative to Information Security.

V. Constraints

Staffing constraint:

- Administrative support for appropriate staffing to support the Information Security Official position
- Staffing within a reasonable period of time
- Staffing to be of trained personnel, or provisions made to supply required training at when hired.

Information Security Official constraint:

- Managerial support for providing an adequately trained ISO to effectively support the HIPAA Security Rules
- Sufficient independence to function without conflict of interest

VI. Dependencies

Appropriate administrative, technical security services, technical security mechanisms, and physical safeguards must be designed to ensure the data integrity, confidentiality, and availability of IIHI and to prevent unauthorized access to data transmitted over a communications network from unintended use or disclosure.

All officials, employers, and employees of the entity must adhere to the entity's policy and procedures regarding security of IIHI. Appropriate sanctions and documentation against violators (including employees) who fail to comply with the entity's security policy and procedures must be applied consistently.

A complaint process must be available, where all complaints are received, documented, and resolved (see Contact Person template).

VII. Process

Covered entities should develop their own processes including specific responsibilities for the Information Security Official representing the covered entity to ensure strict compliance to HIPAA requirements.

VIII. Procedures

A. Preventive measures

The Information Security Official:

Is counsel to new IT application development and hardware/software acquisition to ensure adherence to appropriate security measures.

Performs initial and periodic information security risk assessments and conducts ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.

Works with legal counsel and management, key departments/divisions/sections, and committees to ensure the entity has and maintains appropriate information security functions and materials reflecting current entity's policy and procedures, its legal practices, and requirements.

Develops security standards based on the draft HIPAA Security rule NPRM 142.308 for all trading partner and business associate agreements, to ensure all information security concerns, requirements, and responsibilities are addressed. (See template on Business Associate)

Establishes with management and operations a mechanism to track access to IIHI, within the purview of the entity and as required by law and to allow qualified individuals to review or receive a report on such activity.

B. Guidelines

(1) Policy, Procedures and Training

The Information Security Official:

Provides development guidance and assists in the identification, implementation, and maintenance of the entity's Information Security policy and procedures in coordination with the entity's management, administration, and legal counsel.

Oversees, directs, delivers, or ensures delivery of initial and ongoing Information Security training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties.

Works with the covered entity's organization, legal counsel, and other related parties to represent the entity's Information Security interests with external parties (other state or local government entities) who undertake to adopt or amend Information Security legislation, regulations, or standards.

(2) Public Relations

The Information Security Official:

Increases public's awareness of the organization's efforts to preserve the confidentiality, integrity, and availability of IIHI.

Initiates, facilitates, and promotes activities to foster Information Security awareness within the entity and related entities.

Treats workforce with courtesy, dignity, and respect.

Supports the entity's policy and procedures with a positive image.

(3) Client/ Beneficiary Protections

The Information Security Official:

Requires documented policies and procedures for the receipt, manipulation, storage, dissemination, transmission, and/or disposal of IIHI.

Serves as information security consultant to the enterprise.

(4) Use and Disclosure of IIHI (see Use and Disclosure of Individually Identifiable Health Information template)

The Information Security Official:

Will require the implementation of accurate and current security incident procedures and the establishment of controls to ensure the prevention, detection, containment, and correction of security breaches.

(5) Access

The Information Security Official:

Requires processes to protect information and to control individual access to information by:

Restricting access to resources and allowing access only by authorized entities.

Requiring control mechanisms to assist affected entities identify suspect data access activities, assess its security program, and respond to potential weaknesses.

Requiring entities to be able to provide corroboration that data in its possession has not been altered or destroyed in an unauthorized manner.

Requiring an entity is able to corroborate that the entity is who it claims to be.

Ensures that the entity's Information Security protections keep pace with technological advances.

Collaborates with entity representatives to develop processes to request and authorize computer system access of IIHI for members of the workforce. Citation: Security Rule NPRM 142.308.

(6) Compliance

The Information Security Official:

Ensures compliance with information security practices and consistently applies sanctions for failure (Refer to NPRM section) to comply with information security policy for all individuals in the entity's workforce in cooperation with

Human Resources, other security officials, administration, and legal counsel as applicable.

Cooperates with the Federal Office for Civil Rights, other legal entities, and officials in any compliance reviews or investigations for breeches of Information Security policy and procedures.

(7) Monitoring

The Information Security Official:

Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the entity's information security policy and procedures in coordination and collaboration with other similar functions, and when necessary, legal counsel.

Reviews all system-related Information Security plans throughout the entity's network to ensure alignment between security and Information Security practices, and act as a liaison to the information systems department.

Maintains current knowledge of applicable federal and state Information Security laws and accreditation standards (later applicable to health providers), and monitor advancements in information security technologies to ensure the entity's adaptation and compliance.

(8) Mitigation

The Information Security Official:

In conjunction with the Privacy Official and/or Contact Person, establishes processes to receive, document, and investigate complaints regarding the use and disclosure of IIHI.

Manages individual Information Security disputes and requests for changes to the individual's health information.

In conjunction with the Privacy Official, develops corrective action plans to mitigate harmful effects of inappropriate use or disclosure of IIHI and to decrease the possibility of future breaches of IIHI.

IX. Accessibility of information

This template should be available to every entity that creates or receives IIHI.

X. Compliance criteria

The Information Security Official:

Performs initial and periodic information security risk assessments and conducts ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.

Document security breaches following security incident procedures.

Updates policies and procedures promptly when there is a change in information security law, with approval from security officials, Human Resources, Administration, and Legal Counsel.

XI. Risk (if non-compliant)

Rapid appointment of the Information Security Official enables early Information security risk assessment, effective planning, policy development, training, and implementation.

The entity's administration designates an Information Security Official to be responsible for development and implementation of the entity's policies and procedures for, securing Individually Identifiable Health Information, performance of initial and periodic information security risk assessments, and ongoing compliance monitoring.

The entity provides Information Security training to their entire workforce on its policy and procedures regarding IIHI. After the compliance date, all members of the workforce and business associates who have access to patient information shall receive training in the entity's Information Security policy and procedures, any revisions, and any future changes in Information Security laws. Verification of training must be documented.

There must be procedures in place to mitigate any harmful effect of use or disclosure of IIHI that is a violation of the entity's Information Security practices, policies, or procedures. This includes violations by both members of the workforce and business associates. Administrative requirement is included in Section 164.530 (f) for mitigation.

XII. Auditing Criteria

The Information Security Official:

Provides current versions of security policies and procedures for the covered entity to the U.S. Secretary of Health and Human Services or Office for Civil Rights.

Requires periodic in-house review of the records of system activity to include logins, file accesses, and security incidents.

Requires control mechanisms to help affected entities identify suspect data access activities, assess its security program, and respond to potential weaknesses.

XIII. Template change management process (maintenance)

Information Security Officials, Privacy Officers, Legal Counsel, and the entity's administrative staff should update this template when necessary, and distribute the changes to all members of the workforce, business partners, and other entities as applicable. In addition, they must share such changes and information with those entities that have participated in creating this template.

XIV. Approval policy

A covered entity documents the personnel designations for the Information Security Official.

XV. Disclaimer

The information in this template is for general information only. It is not intended to provide legal advice to any entity. Please consult with your Legal Counsel before taking any action based on information appearing on this template.